Cyclic Codes over Some Finite Quaternion Integer Rings

Mehmet Özen, Murat Güzeltepe
Department of Mathematics, Sakarya University, TR54187 Sakarya, Turkey

Abstract

In this paper, cyclic codes are established over some finite quaternion integer rings with respect to the quaternion Mannheim distance, and decoding algorithm for these codes is given.

2000 AMS Classification: 94B05, 94B15, 94B35, 94B60
Keywords: Block codes, Mannheim distance, Cyclic codes, Syndrome decoding

1 Introduction

Mannheim distance, which is much better suited for coding over two dimensional signal space than the Hamming distance, was introduced by Huber [1]. Moreover, Huber constructed one Mannheim error correcting codes, which are suitable for quadrature amplitude modulation (QAM)-type modulations [1]. Cyclic codes over some finite rings with respect to the Mannheim metric were obtained by using Gaussian integers in [2]. Later, in [3], using quaternion Mannheim metric, also called Lipschitz metric [4], perfect codes over some finite quaternion integer rings were obtained and these codes were decoded.

The rest of this paper is organized as follows. In Section II, quaternion integers and some fundamental algebraic concepts have been considered. In Section III, we construct cyclic codes over some quaternion integer rings with respect to quaternion Mannheim metric.

2 Quaternion Integers

Definition 1 *The Hamilton Quaternion Algebra over the set of the real numbers ($\mathcal{R}$), denoted by $H(\mathcal{R})$, is the associative unital algebra given by the following representation:*

i)$H(\mathcal{R})$ is the free $\mathcal{R}$ module over the symbols $1, i, j, k$, that is, $H(R) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in R\}$;

ii)1 is the multiplicative unit;

iii) $i^2 = j^2 = k^2 = -1$;

iv) $ij = -ji = k$, $ik = -ki = j$, $jk = -kj = i$ [5].

The set $H(\mathcal{Z})$, $H(\mathcal{Z}) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in \mathcal{Z}\}$, is a subset of $H(\mathcal{R})$, where $\mathcal{Z}$ is the set of all integers. If $q = a_0 + a_1 i + a_2 j + a_3 k$ is

a quaternion integer, its conjugate quaternion is $\overline{q} = a_0 - (a_1 i + a_2 j + a_3 k)$.The norm of q is $N(q) = q.\overline{q} = a_0^2 + a_1^2 + a_2^2 + a_3^2$. A quaternion integer consists of two parts which are the complete part and the vector part. Let $q = a_0 + a_1 i + a_2 j + a_3 k$ be a quaternion integer. Then its complete part is a_0 and its vector part is $a_1 i + a_2 j + a_3 k$. The commutative property of multiplication does not hold for quaternion integers. However, if the vector parts of quaternion integers are parallel to each other, then their product is commutative. Define $H(K_1)$ as follows:

$$H(K_1) = \{a_0 + a_1(i + j + k) : \ a_0, a_1 \in Z\}$$

which is a subset of quaternion integers. The commutative property of multiplication holds over $H(K_1)$.

Theorem 1 *For every odd, rational prime $p \in \mathcal{N}$, there exists a prime $\pi \in H(\mathcal{Z})$, such that $N(\pi) = p = \pi\overline{\pi}$. In particular, p is not prime in $H(Z)$ [5].*

Corollary 1 *$\pi \in H(\mathcal{Z})$ is prime in $H(\mathcal{Z})$ if and only if $N(\pi)$ is prime in $\mathcal{Z}$ [5].*

Theorem 2 *If a and b are relatively prime integers then $H(K_1)/\langle a + b(i + j + k)\rangle$ is isomorphic to $Z_{a^2+3b^2}$ [3, 5, 7].*

3 Cyclic Codes over Quaternion Integer Rings

Let $H(K_1)_{\pi^k}$ be the residue class of $H(K_1)_\pi$ modulo π^k, where k is any positive integer and π is a prime quaternion integer. According to the modulo function $\mu : \mathcal{Z}_{P^k} \to H(K_1)_{\pi^k}$ defined by

$$g \to g - [\frac{g.\overline{\pi}}{\pi.\overline{\pi}}]\pi \ (\mathrm{mod}\pi^k) \tag{1}$$

$H(K_1)_{\pi^k}$ is isomorphic to Z_{p^k}, where $p = \pi\overline{\pi}$ and p is an odd prime. A quaternion cyclic codes C of length n is a linear code C of length n with property

$$(c_0, c_1, ..., c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, c_1, ..., c_{n-2}) \in C.$$

In this case, we have a bijective

$$\begin{array}{cc} H(K_1)^n_{\pi^k} \to H(K_1)_{\pi^k}[x]/(x^n - 1) \\ (c_0, c_1, ..., c_{n-1}) \qquad \mapsto c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + (x^n - 1) \end{array} \tag{2}$$

To put it simply, we write $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ for $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + (x^n - 1)$. A nonempty set of $H(K_1)^n_{\pi^k}$ is a $H(K_1)_{\pi^k}$-cyclic code if and only if its image under (2) is an ideal of $H(K_1)_{\pi^k}[x]/(x^n - 1)$. More information on cyclic codes can be found in [6].

Definition 2 *Let $\alpha, \beta \in H(K_1)_\pi$ and $\gamma = \beta - \alpha = a + b(i + j + k)$ $(\mathrm{mod}\pi)$, where π is a prime quaternion integer. Let the quaternion Mannheim weight of γ be defined as*

$$w_{QM}(\gamma) = |a| + 3\,|b|$$

the quaternion Mannheim distance d_{QM} between α and β is defined as

$$d_{QM}(\alpha, \beta) = w_{QM}(\gamma).[\beta]$$

Proposition 1 *Let $\pi = a + b(i + j + k)$ be a prime in the set $H(K_1)$ and let $p = a^2 + 3b^2$ be prime in $\mathcal{Z}$. If g is a generator of $H(K_1)^*_{\pi^2}$, then $g^{\phi(p^2)/2} \equiv -1 \pmod{\pi^2}$.*

Proof. If $N(\pi)$ is a prime integer in $\mathcal{Z}$, then the complete part and the coefficient of the vector part of π^2 are relatively integer. So, $\mathcal{Z}_{p^2}$ is isomorphic to $H(K_1)_{\pi^2}$ (See Theorem 2). If g is a generator of $H(K_1)^*_{\pi^2}$, then g, g^2, ..., $g^{\phi(p^2)}$ constitute a reduced residue system modulo π^2 in $H(K_1)_{\pi^2}$. Therefore, there is a positive integer k as $g^k \equiv -1 \pmod{\pi^2}$, where $1 \leq k \leq \phi(p^2)$. Hence, we can infer $g^{2k} \equiv 1 \pmod{\pi^2}$. Since $\phi(p^2) \big| 2k$ and $2 \leq 2k \leq 2\phi(p^2)$, we obtain $\phi(p^2) = k$ or $\phi(p^2) = 2k$. If $\phi(p^2)$ was equal to k, we should have $\pi^2 \big| 2$, but this would contradict the fact that $N(\pi^2) > 2$. ■

Proposition 2 *Let $\pi_k = a_k + b_k(i + j + k)$ be distinct primes in $H(K_1)$ and let $p_k = a_k^2 + 3b_k^2$ be distinct primes in $\mathcal{Z}$, where $k = 1, 2, ..., m$. If g is a generator of $H(K_1)^*_{\pi^k}$, then $g^{\phi(p^k)/2} \equiv -1 \pmod{\pi^k}$.*

Proof. This is certain from Proposition 1. ■

Theorem 3 *Let $\pi = a + b(i + j + k)$ be a prime in $H(K_1)$ and let $p = a^2 + 3b^2$ be a prime in $\mathcal{Z}$, where $a, b \in \mathcal{Z}$. Then, cyclic codes whose lengths are $\phi(p^2)/2$ are obtained.*

Proof. $H(K_1)^*_{\pi^2}$ has a generator since $\mathcal{Z}_{p^2} \cong H(K_1)_{\pi^2}$. Let the generator be g. Then we get $g^{\phi(p^2)} = 1$ and $g^{\phi(p^2)/2} = -1$. Hence, we can write

$$x^{\phi(p^2)/2} + 1 = (x - g)Q(x) \pmod{\pi^2} \text{ (for } x = g).$$

In this situation, $(x - g)$ is an ideal of $H(K_1)_{\pi^2}[x] \Big/ \left\langle x^{\phi(p^2)/2} + 1 \right\rangle$, i.e., it generates a cyclic code. ■

If the generator polynomial is taken as a monic polynomial, all components of any row of the generator matrix do not consist of zero divisors. Therefore, these codes are free $H(K_1)_{\pi^2}$ modules.

Proposition 3 *Let $\pi_1 = a+b(i+j+k)$, $\pi_2 = c+d(i+j+k)$ be primes in $H(K_1)$ and let $p_1 = a^2+3b^2$, $p_2 = c^2+3d^2$ be primes in $\mathcal{Z}$. Then, there are two elements of $H(K_1)^*_{\pi_1\pi_2}$ such that $e^{\phi(p_2)} \equiv 1 \pmod{\pi_1\pi_2}$ and $f^{\phi(p_1)} \equiv 1 \pmod{\pi_1\pi_2}$.*

Proof. Since p_1 and p_2 are relatively prime integers in $\mathcal{Z}$, π_1 and π_2 are relatively primes in $H(K_1)$. Using the basic algebraic knowledge and the function (1), we get $\mathcal{Z}_{p_1} \cong H(K_1)_{\pi_1}$, $\mathcal{Z}_{p_2} \cong H(K_1)_{\pi_2}$ and $\mathcal{Z}_{p_1p_2} \cong H(K_1)_{\pi_1\pi_2}$. Moreover, we obtain as follows:

$$H(K_1)^*_{\pi_1\pi_2}(\pi_1) \cong \mathcal{Z}^*_{p_1p_2}(p_1) \cong \mathcal{Z}^*_{p_2} \cong H(K_1)^*_{\pi_2},$$

$$H(K_1)^*_{\pi_1\pi_2}(\pi_2) \cong \mathcal{Z}^*_{p_1p_2}(p_2) \cong \mathcal{Z}^*_{p_1} \cong H(K_1)^*_{\pi_1}.$$

Since π_2 is a prime quaternion integer, $H(K_1)^*_{\pi_2}$ is a cyclic group. Therefore, $H(K_1)^*_{\pi_2}$ has a generator. So, $H(K_1)^*_{\pi_1\pi_2}(\pi_1)$ has a generator, either. Let the generator be e. Then $e^{\phi(p_2)} \equiv 1 \pmod{\pi_1\pi_2}$. In the same way, $H(K_1)^*_{\pi_1\pi_2}(\pi_2)$ has a generator. Suppose that f is the generator of $H(K_1)^*_{\pi_1\pi_2}(\pi_2)$. Then $f^{\phi(p_1)} \equiv 1 \pmod{\pi_1\pi_2}$. ■

Proposition 4 *Let $\pi_k = a_k + b_k(i+j+k)$ be a prime in $H(K_1)$ and let $p_k = a_k^2 + 3b_k^2$ be distinct odd primes in $\mathcal{Z}$. Then, there is an element e_k of $H(K_1)^*_{\pi_1\pi_2...\pi_k}$ such that $e_k^{\phi(p_k)} \equiv 1 \ (\mathrm{mod}\pi_1\pi_2...\pi_k)$, $k = 1, 2, ..., m$.*

Proof. This is clear from Proposition 3. ■

Theorem 4 *Let $\pi_1 = a+b(i+j+k)$, $\pi_2 = c+d(i+j+k)$ be primes in $H(K_1)$ and let $p_1 = a^2+3b^2$, $p_2 = c^2+3d^2$ be odd primes in $\mathcal{Z}$. Then, we can always write cyclic codes of length $\phi(p_1)$ and $\phi(p_2)$ over $H(K_1)_{\pi_1\pi_2}$.Moreover, the generator polynomials of these codes are first degree monic polynomials. Therefore, these codes are free $H(K_1)_{\pi_1\pi_2}$ module.*

Proof. From Proposition 3, we can find an element of $H(K_1)_{\pi_1\pi_2}$ such that $e^{\phi(p_2)} \equiv 1 \ (\mathrm{mod}\pi_1\pi_2)$. Thus, we factorize the polynomial $x^{\phi(p_2)} - 1$ over $H(K_1)_{\pi_1\pi_2}$ as $x^{\phi(p_2)} - 1 = (x-e)D(x)(\mathrm{mod}\pi_1\pi_2)$. If we take the generator polynomial as $g(x) = x - e$, then the generator polynomial $g(x)$ forms the generator matrix whose all components of any rows do not consist of zero divisors. ■

We now consider a simple example with regard to Theorem 3.

Example 1 *Let π be $2+i+j+k$. The polynomial $x^{21}+1$ factors over $H(K_1)_{\pi^2}$ as $x^{21}+1 = (x-\alpha).(x^{20} + \alpha x^{19} + \alpha^2 x^{18} + \alpha^3 x^{17} + ... + \alpha^{19}x + \alpha^{20})$, where $\alpha = 1-i-j-k$. The powers of α are shown in Table I. If we choose the generator polynomial as $g(x) = x - \alpha$, then the generator matrix is as follows:*

$$G = \begin{pmatrix} -\alpha & 1 & 0 & 0 & \cdots & 0 \\ 0 & -\alpha & 1 & 0 & \cdots & 0 \\ 0 & 0 & -\alpha & 1 & \ddots & 0 \\ \vdots & \vdots & & \ddots & \ddots & \\ 0 & 0 & \cdots & 0 & -\alpha & 1 \end{pmatrix}_{20\text{x}21} .$$

The code C generated by the generator matrix G can correct one error having quaternion Mannheim weight of one.

Table I: Powers of the element $\alpha = 1-i-j-k$ which is root of x^3+1.

s	α^s	s	α^s	s	α^s	s	α^s
0	1	6	$3+i+j+k$	12	$4-2i-2j-2k$	18	-6
1	$1-i-j-k$	7	$-6-i-j-k$	13	$2i+2j+2k$	19	$5+i+j+k$
2	$-1+2i+2j+2k$	8	2	14	$5-2i-2j-2k$	20	$-3+i+j+k$
3	$4-i-j-k$	9	$2-2i-2j-2k$	15	$1+i+j+k$	21	-1
4	$2-i-j-k$	10	-3	16	4	22	$-\alpha = -1+i+j+k$
5	$i+j+k$	11	$-4-i-j-k$	17	5	23	$-\alpha^2 = 1-2i-2j-2k$

References

[1] Huber K., "Codes Over Gaussian Integers" IEEE Trans. Inform.Theory, vol. 40, pp. 207-216, Jan. 1994.

[2] M. Özen and M. Güzeltepe, "Cyclic Codes over Some Finite Rings" (Submitted 2009).

[3] M. Özen and M. Güzeltepe, "Codes over Quaternion Integers" (Submitted 2009).

[4] C. Martinez, E. Stafford, R. Beivide, E. Gabidulin, "Perfect Codes over Lipschitz Integers" IEEE Int. Symposium, ISIT 2007.

[5] G. Davidoff, P. Sarnak, A. Valette, "Elementary Number Theory, Group Theory, Ramanujan Graphs", Cambridge University Pres, 2003.

[6] F. J. Macwilliams and N. J. SLOANE, "The Theory of Error Correcting Codes", North Holland Pub. Co., 1977 .

[7] G. Dresden and W. M. Dymacek, "Finding Factors of Factor Rings over the Gaussian Integers" The Mathematical Association of America, Monthly Aug-Sep. 2005.

[8] I. Ziven, H.S. Zuckerman and H.L. Montgomery, "An Introduction to the Number Theory" John Wiley and Sons, Inc., 1991.